

Exhibit A

[Click here to Respond to Selected Documents](#)

Sort Date Entries: Descending Ascending

Display Options: All Entries 

06/02/2025

Summons Issued-Circuit

Document ID: 25-SMCC-8933, for AMERICAN MULTISPECIALTY GROUP, INC. Summons Attached in PDF Form for Attorney to Retrieve from Secure Case.Net and Process for Service.

05/29/2025

Filing Info Sheet eFiling

Filed By: JOHN FRANCIS GARVEY JR

Motion Special Process Server

Request for Appointment of Special Process Server.

Filed By: JOHN FRANCIS GARVEY JR

On Behalf Of: ROBIN WILLIS

Pet Filed in Circuit Ct

Class Action Petition.

Filed By: JOHN FRANCIS GARVEY JR

On Behalf Of: ROBIN WILLIS

Judge Assigned

DIV 7

IN THE CIRCUIT COURT OF ST. LOUIS COUNTY
STATE OF MISSOURI

ROBIN WILLIS, individually and on behalf of
all others similarly situated,

Plaintiff,

v.

AMERICAN MULTISPECIALTY GROUP,
INC. d/b/a ESSE HEALTH,

Serve: 12655 Olive Blvd., 4th Floor
St. Louis, MO 63141

Defendant.

Case No.

Division No.

JURY TRIAL DEMANDED

CLASS ACTION PETITION

Plaintiff Robin Willis (“Plaintiff”) brings this Class Action Complaint (“Complaint”) against American Multispecialty Group, Inc. d/b/a/ Esse Health (“Esse” or “Defendant”) as an individual and on behalf of all others similarly situated. Plaintiff alleges, upon personal knowledge as to her own actions and her counsels’ investigation, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted Defendant with sensitive Personally Identifiable Information (“PII”)¹ and Protected Health Information (“PHI”) (collectively, “Private Information”) that was impacted in a data breach that occurred in late April 2025 (the “Data Breach” or the “Breach”).

¹ Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

2. Plaintiff's claims arise from Defendant's failure to properly secure and safeguard Private Information that was entrusted to it, and its accompanying responsibility to store and transfer that information.

3. Defendant is an independent physician group healthcare provider with 50 locations in the Greater St. Louis area in Missouri.²

4. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to Plaintiff and Class Members, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

5. In late April 2025, Defendant detected unusual activity on its IT Network.³ The Data Breach caused Defendant's network systems to be taken offline.⁴ In response to the incident, Defendant launched an investigation to determine the nature and scope of the Data Breach.⁵

6. Defendant admits that information in its system was accessed by an unauthorized actor, though it has provided little information regarding how the Data Breach occurred.⁶

7. Defendant failed to take precautions designed to keep individuals' Private Information secure.

8. Defendant owed Plaintiff and Class Members a duty to take all reasonable and necessary measures to keep the Private Information collected safe and secure from unauthorized access. Defendant solicited, collected, used, and derived a benefit from the Private Information, yet breached its duty by failing to implement or maintain adequate security practices.

² *About Us*, American Multispecialty Group, Inc. d/b/a Esse Health <https://www.essehealth.com/about-us/> (last visited May 20, 2025).

³ <https://www.hipaajournal.com/esse-health-cyberattack/> (last visited May 20, 2025).

⁴ *Id.*

⁵ *Id.*

⁶ *Id.*

9. The sensitive nature of the data maintained by Defendant and potentially compromised in the Data Breach, signifies that Plaintiff and Class Members have suffered irreparable harm. Plaintiff and Class Members have lost the ability to control their Private Information and are subject to an increased risk of identity theft.

10. Defendant, despite having the financial wherewithal and personnel necessary to prevent the Data Breach, nevertheless failed to use reasonable security procedures and practice appropriate to the nature of the sensitive, unencrypted information it maintained for Plaintiff and Class Members, causing the exposure of Plaintiff's and Class Members' Private Information.

11. As a result of Defendant's inadequate digital security and notice process, Plaintiff's and Class Members' Private Information was exposed to criminals. Plaintiff and the Class Members have suffered and will continue to suffer injuries including: financial losses caused by misuse of their Private Information; the loss or diminished value of their Private Information as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal and financial information.

12. Moreover, as an ongoing harm resulting from the Data Breach, Plaintiff and Class Members experienced disruptions in services because Defendant's IT Network went offline. These disruptions included delays in obtaining treatment, cancellation of medical appointments with providers, and inability to schedule medical appointments.

13. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; (iii) effectively secure hardware containing protected Private Information using reasonable and adequate security procedures free of vulnerabilities and

incidents; and (iv) timely notify Plaintiff and Class Members of the Data Breach. Defendant's conduct amounts to at least negligence and violates federal and state statutes.

14. Plaintiff brings this action against Defendant for: negligence, negligence *per se*, unjust enrichment, breach of implied contract, breach of confidence, invasion of privacy, and violation of the Missouri Merchandise Practices Act, Mo. Rev. Stat. §§ 407.010, *et seq.*

15. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of herself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

JURISDICTION AND VENUE

16. The Court has jurisdiction over the parties because Defendant is a Missouri based corporation that can be found and served in the State of Missouri and regularly conducts business in the State.

17. Venue is proper because Defendant has its principal place of business within the State in St. Louis County.

PARTIES

18. Plaintiff Robin Willis is, and was at all times relevant to this litigation, a resident and citizen of St. Louis, Missouri.

19. Defendant is a corporation organized under the laws of the State of Missouri with its principal place of business located at 12655 Olive Boulevard, Floor 4, Saint Louis, Missouri, 63141.

FACTUAL ALLEGATIONS

Defendant Esse Health

20. Plaintiff and Class Members are current/former patients of Defendant.

21. Defendant is an independent physician group healthcare provider with 50 locations in the Greater St. Louis area in Missouri.

22. Upon information and belief, Defendant made promises and representations to individuals, including Plaintiff and Class Members, that the Private Information collected from them would be kept safe and confidential, and that the privacy of that information would be maintained.⁷

23. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

24. As a result of collecting and storing the Private Information of Plaintiff and Class Members for its own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiff's and the Class Members' Private Information from disclosure to third parties.

Defendant's Data Breach

25. In late April 2025, Defendant detected unusual activity on its IT Network.⁸ The Data Breach caused Defendant's network systems to be taken offline.⁹

26. In response to the incident, Defendant launched an investigation to determine the nature and scope of the Data Breach.¹⁰

27. As a result of the Data Breach, numerous patients reported that their healthcare was placed on hold, with medical appointments and scheduling delays occurring.¹¹

⁷ Privacy Policy, American Multispecialty Group, Inc. d/b/a Esse Health <https://www.essehealth.com/privacy-policy/> (last visited May 20, 2025).

⁸ <https://www.hipaajournal.com/esse-health-cyberattack/> (last visited May 20, 2025).

⁹ *Id.*

¹⁰ *Id.*

¹¹ <https://healthexec.com/topics/health-it/cybersecurity/independent-provider-group-hit-cyberattack-delays-patient-care> (last visited May 20, 2025).

28. Defendant admits that information in its system was accessed by an unauthorized actor, though it has provided little information regarding how the Data Breach occurred.¹²

29. Plaintiff's claims arise from Defendant's failure to safeguard Private Information provided by and belonging to its patients and failure to provide timely notice of the Data Breach.

30. Defendant failed to take precautions designed to keep its patients' Private Information secure.

31. While Defendant sought to minimize the damage caused by the Data Breach, it cannot and has not denied that there was unauthorized access to the sensitive Private Information of Plaintiff and Class Members.

32. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

33. Defendant admits that an unauthorized third party accessed its IT Network. Defendant failed to take adequate measures to protect its computer systems against unauthorized access.

34. The Private Information that Defendant allowed to be exposed in the Data Breach is the type of private information that Defendant knew or should have known would be the target of cyberattacks.

35. Defendant was not only aware of the importance of protecting the Private Information that it maintains, as alleged, it promoted its capability to do so, as evident from its Privacy Policy.¹³

¹² *Id.*

¹³ *Privacy Policy*, American Multispecialty Group, Inc. d/b/a Esse Health <https://www.essehealth.com/privacy-policy/> (last visited May 14, 2025).

36. Despite its own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,¹⁴ Defendant failed to disclose that its systems and security practices were inadequate to reasonably individuals' Private Information.

37. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.¹⁵ Immediate notification of a Data Breach is critical so that those impacted can take measures to protect themselves.

38. Here, Defendant has yet to directly notify impacted individuals of the Data Breach.

Data Breaches Are Preventable

39. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

40. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

41. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."¹⁴

42. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

¹⁴ How to Protect Your Networks from RANSOMWARE, at 3, available at: <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical

separation of networks and data for different organizational units.¹⁵

43. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface]

¹⁵ *Id.* at 3-4.

for Office [Visual Basic for Applications].¹⁶

44. Given that Defendant was storing the Private Information of its current and former patients, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

45. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and data thieves acquiring and accessing the Private Information of more than fifty thousand individuals, including that of Plaintiff and Class Members.

Defendant Acquires, Collects, And Stores Its Patient's Private Information

46. Defendant acquires, collects, and stores a massive amount of Private Information on its current and former patients.

47. As a condition of obtaining medical services from Defendant, Defendant requires that patients entrust it with highly sensitive personal information.

48. By obtaining, collecting, and using Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

49. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and would not have entrusted it to Defendant absent a promise to safeguard that information.

¹⁶ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at*: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>

50. Upon information and belief, in the course of collecting Private Information from patients, including Plaintiff, Defendant promised to provide confidentiality and adequate security for their data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

51. Plaintiff and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Value Of Personally Identifying Information

52. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”¹⁷ The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”¹⁸

53. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.¹⁹

¹⁷ 17 C.F.R. § 248.201 (2013).

¹⁸ *Id.*

¹⁹ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>

54. For example, Personal Information can be sold at a price ranging from \$40 to \$200.²⁰ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.²¹

55. Moreover, Social Security numbers are among the worst kind of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

56. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases."²² Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."²³

57. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and some Class Members, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone

²⁰ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>

²¹ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>

²² *See*

<https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases.>

²³ *Id.*

illegally using your Social Security number and assuming your identity can cause a lot of problems.²⁴

58. In fact, “[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health.”²⁵ “Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits.”²⁶

59. What’s more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

60. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, “[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”²⁷

61. For these reasons, some courts have referred to Social Security numbers as the “gold standard” for identity theft. *Portier v. NEO Tech. Sols.*, No. 3:17-CV-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) (“Because Social Security numbers are the gold standard for identity theft, their theft is significant Access to Social Security numbers causes long-

²⁴ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf>

²⁵ See <https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/>

²⁶ See <https://www.investopedia.com/terms/s/ssn.asp>

²⁷ Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft>

lasting jeopardy because the Social Security Administration does not normally replace Social Security numbers.”), report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *see also* *McFarlane v. Altice USA, Inc.*, 2021 WL 860584, at *4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiff’s Social Security numbers are: arguably “the most dangerous type of personal information in the hands of identity thieves” because it is immutable and can be used to “impersonat[e] [the victim] to get medical services, government benefits, ... tax refunds, [and] employment.” . . . Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, “[a] social security number derives its value in that it is immutable,” and when it is stolen it can “forever be wielded to identify [the victim] and target him in fraudulent schemes and identity theft attacks.”)

62. Similarly, the California state government warns consumers that: “[o]riginally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job.”²⁸

63. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”²⁹

²⁸ See <https://oag.ca.gov/idtheft/facts/your-ssn>

²⁹ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>

64. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

65. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.³⁰

66. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

Defendant Fails To Comply With FTC Guidelines

67. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

68. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer

³⁰ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf>

networks; understand their network's vulnerabilities; and implement policies to correct any security problems.³¹

69. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.³²

70. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

71. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

72. These FTC enforcement actions include actions against entities that maintain PHI like Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (Henry Ford) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that

³¹ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

³² *Id.*

LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

73. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

74. Defendant failed to properly implement basic data security practices.

75. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to the Private Information of its patients or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

76. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

Defendant Fails To Comply With Industry Standards

77. As noted above, experts studying cyber security routinely identify entities in possession of large amounts of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

78. Several best practices have been identified that, at a minimum, should be implemented by these entities in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Leaders Staffing failed to follow these industry best practices, including a failure to implement multi-factor authentication.

79. Other best cybersecurity practices that are standard for entities include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Leaders Staffing failed to follow these cybersecurity best practices, including failure to train staff.

80. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

81. These foregoing frameworks are existing and applicable industry standards for similar entities, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Common Injuries & Damages

82. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

Data Breaches Cause Disruptions That Put Patients at an Increased Risk of Harm

83. Cyber-attacks at medical facilities such as Defendant's are especially problematic because of the disruption they cause to the health treatment and overall daily lives of patients affected by the attack.

84. For instance, loss of access to patient histories, charts, images, and other information forces providers to limit or cancel patient treatment due to a disruption of service. This leads to a deterioration in the quality of overall care patients receive at facilities affected by cyber-attacks and related data breaches.

85. Researchers have found medical facilities that experience a data security incident incur an increase in the death rate among patients' months and years after the attack.³³ Researchers have further found that at medical facilities that experience a data breach, the incident leads to a deterioration in patient outcomes, generally.³⁴

86. Similarly, cyber-attacks and related data security incidents inconvenience patients; these inconveniences include, but are not limited, to the following:

- a. rescheduling of medical treatment;
- b. being forced to find alternative medical care and treatment;
- c. delays or outright cancellation of medical care and treatment;
- d. undergoing medical care and treatment without medical providers having access to a complete medical history and records; and
- e. the indefinite loss of personal medical history.

Data Breaches Increase Victims' Risk Of Identity Theft

87. The unencrypted Private Information of Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

88. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Simply put, unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

³³ See Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019) <https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks> (last visited May 20, 2025).

³⁴ See Sung J. Choi PhD., et al., *Data breach remediation efforts and their implications for hospital quality*, HEALTH SERVICES RESEARCH (Sept. 10, 2019) <https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203> (last visited May 20, 2025).

89. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

90. Plaintiff's and Class Members' Private Information is of great value to hackers and cyber criminals. As a result of the Data Breach, the Private Information of Plaintiff and Class Members has been exposed to criminals for misuse.

91. Due to the risk of one's Social Security number being exposed, state legislatures have passed laws in recognition of the risk: "[t]he social security number can be used as a tool to perpetuate fraud against a person and to acquire sensitive personal, financial, medical, and familial information, the release of which could cause great financial or personal harm to an individual. While the social security number was intended to be used solely for the administration of the federal Social Security System, over time this unique numeric identifier has been used extensively for identity verification purposes[.]"³⁵

92. Moreover, "SSNs have been central to the American identity infrastructure for years, being used as a key identifier[.] . . . U.S. banking processes have also had SSNs baked into their identification process for years. In fact, SSNs have been the gold standard for identifying and verifying the credit history of prospective employees."³⁶

93. "Despite the risk of fraud associated with the theft of Social Security numbers, just five of the nation's largest 25 banks have stopped using the numbers to verify a employee's identity

³⁵ See N.C. Gen. Stat. § 132-1.10(1).

³⁶ See <https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers>

after the initial account setup[.]”³⁷ Accordingly, since Social Security numbers are frequently used to verify an individual’s identity after logging onto an account or attempting a transaction, “[h]aving access to your Social Security number may be enough to help a thief steal money from your bank account”³⁸

94. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of “Fullz” packages.³⁹

95. With “Fullz” packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

96. The development of “Fullz” packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff’s and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other

³⁷ See <https://archive.nytimes.com/bucks.blogs.nytimes.com/2013/03/20/just-5-banks-prohibit-use-of-social-security-numbers/>

³⁸ See <https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>

³⁹ “Fullz” is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. See, e.g., Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), [https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-\]\(https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-/)

words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

97. The existence and prevalence of “Fullz” packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like insurance information) of Plaintiff and the other Class Members.

98. Thus, even if certain information (such as insurance information) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

99. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate Risk Of Identity Theft & Fraud

100. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

101. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach. Accordingly, the Data Breach has caused Plaintiff and Class Members to suffer actual injury in the form of lost time—which cannot be recaptured—spent on mitigation activities.

102. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."⁴⁰

103. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.⁴¹

104. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."^[4]

Diminution of Value of Private Information

105. Private Information and PHI are valuable property rights.⁴² Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

⁴⁰ See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

⁴¹ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps>

⁴² See "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> ("GAO Report").

106. Sensitive Private Information can sell for as much as \$363 per record according to the Infosec Institute.⁴³

107. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly \$200 billion.⁴⁴

108. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.^{45,46}

109. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.⁴⁷

110. Theft of PHI is also gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”⁴⁸

111. As a result of the Data Breach, Plaintiff’s and Class Members’ Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred

⁴³ See, e.g., John T. Soma, et al, Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“Private Information”) Equals the “Value” of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) (“Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

⁴⁴ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>

⁴⁵ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

⁴⁶ <https://datacoup.com/>

⁴⁷ <https://digi.me/what-is-digime/>

⁴⁸ *Medical I.D. Theft*, EFraudPrevention

<https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected.> (last visited Nov. 6, 2023).

without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

112. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

113. The fraudulent activity resulting from the Data Breach may not come to light for years.

114. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

115. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network and, as a result, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

116. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

117. Given the type of targeted attack in this case, sophisticated criminal activity, and the type of Private Information involved, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and

purchase by criminals intending to utilize the Private Information for identity theft crimes –e.g., opening bank accounts in the victims’ names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

118. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual’s employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual’s authentic tax return is rejected.

119. Consequently, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

120. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

Plaintiff Robin Willis’ Experience

121. Plaintiff is a current patient of Defendant.

122. As a condition of obtaining medical services from Defendant, she was required to provide her Private Information to Defendant, including her name, date of birth, Social Security number, medical information, and health insurance information.

123. At the time of the Data Breach, Defendant maintained Plaintiff’s Private Information in its system.

124. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any

other unsecured source. Plaintiff would not have entrusted her Private Information to Defendant had he known of Defendant's lax data security policies.

125. Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

126. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

127. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not informed her of key details about the Data Breach's occurrence.

128. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

129. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

130. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

131. Plaintiff brings this class action on behalf of herself and on behalf of the following class:

All persons who were impacted by the Data Breach announced by Defendant in April 2025 (the "Class").

132. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

133. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

134. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable. Upon information and belief, there are thousands of individuals whose Private Information may have been improperly accessed in the Data Breach. The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

135. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the

questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

- a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;
- b. Whether Defendant had respective duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant had respective duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;
- e. Whether and when Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;
- h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

- k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

136. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

137. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenges of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

138. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intend to prosecute this action vigorously.

139. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and

expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

140. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

141. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

142. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

143. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to

provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

144. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

145. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant failed to timely notify the Plaintiff and the class of the Data Breach;
- b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;
- c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;
- d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT I

Negligence

(On Behalf of Plaintiff and the Class)

146. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

147. Plaintiff realleges all previous paragraphs as if fully set forth below.

148. Plaintiff and members of the Class entrusted their Private Information to Defendant. Defendant owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the Private Information in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use, and to promptly detect attempts at unauthorized access.

149. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their Private Information in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that Private Information—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff and members of the Class's Private Information by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

150. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their Private Information. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope,

nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

151. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff and members of the Class's personal information and Private Information.

152. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that Defendant holds vast amounts of Private Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Private Information—whether by malware or otherwise.

153. Private Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiff and members of the Class's and the importance of exercising reasonable care in handling it.

154. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

155. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

156. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's Private Information.

157. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, patients' Private Information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the members of the Class's sensitive Private Information.

158. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its patients' Private Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its patients in the event of a breach, which ultimately came to pass.

159. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

160. Defendant had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Class's Private Information.

161. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's Private Information.

162. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

163. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

164. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their Private Information.

165. Had Plaintiff and members of the Class known that Defendant did not adequately protect their Private Information, Plaintiff and members of the Class would not have entrusted Defendant with their Private Information.

166. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and members of the Class have suffered harm, including loss of time and money obtaining protections against future identity theft; lost control over the value of Private Information; and other harms resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT III
Breach of an Implied Contract
(On Behalf of Plaintiff and the Class)

167. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

168. Defendant offered medical services to Plaintiff and members of the Class in exchange for their Private Information and payment.

169. In turn, Defendant agreed it would not disclose the Private Information it collects to unauthorized persons. Defendant also promised to safeguard patient Private Information.

170. Plaintiff and the members of the Class accepted Defendant's offer by providing Private Information and payment to Defendant in exchange for medical services.

171. Implicit in the parties' agreement was that Defendant would provide Plaintiff and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their Private Information.

172. Plaintiff and the members of the Class would not have entrusted their Private Information to Defendant in the absence of such agreement with Defendant.

173. Defendant materially breached the contract(s) it had entered with Plaintiff and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant further breached the implied contracts with Plaintiff and members of the Class by:

- i. Failing to properly safeguard and protect Plaintiff and members of the Class's Private Information;
- ii. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and
- iii. Failing to ensure the confidentiality and integrity of electronic Private

Information that Defendant created, received, maintained, and transmitted.

174. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

175. Plaintiff and members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

176. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

177. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

178. Defendant failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

179. In these and other ways, Defendant violated its duty of good faith and fair dealing.

180. Plaintiff and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

181. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

182. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

183. Plaintiff and members of the Class conferred a benefit upon Defendant in the form of payment and providing Private Information.

184. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Class. Defendant also benefited from the receipt of Plaintiff and members of the Class's Private Information, as this was used to facilitate their payment for medical services.

185. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the proposed Class's services and their Private Information because Defendant failed to adequately protect their Private Information. Plaintiff and the proposed Class would not have provided their Private Information or paid Defendant had they known Defendant would not adequately protect their Private Information.

186. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

COUNT V
BREACH OF CONFIDENCE
(On behalf of Plaintiffs and the Class)

146. Plaintiffs and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

147. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Private Information that Plaintiff and Class Members entrusted to Defendant.

148. As alleged herein and above, Defendant's relationship with Plaintiff and the Class was governed by terms and expectations that Plaintiff's and the Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

149. Plaintiff and the Class entrusted Defendant with their Private Information with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized third parties.

150. Plaintiff and the Class also entrusted Defendant with their Private Information with the explicit and implicit understandings that Defendant would take precautions to protect that Private Information from unauthorized disclosure.

151. Defendant voluntarily received Plaintiff's and Class Members' Private Information in confidence with the understanding that their Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

152. As a result of Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

153. As a direct and proximate cause of Defendant's actions and omissions, Plaintiff and the Class have suffered damages.

154. But for Defendant's disclosure of Plaintiff's and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' Private Information as well as the resulting damages.

155. The injury and harm Plaintiff and the Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' Private Information. Defendant knew or should have known its methods of accepting and securing Plaintiff's and Class Members' Private Information was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and Class Members' Private Information.

156. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Class, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized

disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of individuals; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

157. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT VI
INVASION OF PRIVACY
(On Behalf of Plaintiffs and Class)

158. Plaintiffs and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

159. Plaintiffs and the Class had a legitimate expectation of privacy to their Private Information and were entitled to the protection of this information against disclosure to unauthorized third parties.

160. Defendant owed a duty to its current and former patients, including Plaintiffs and the Class, to keep their Private Information contained as a part thereof, confidential.

161. Defendant failed to protect and released to unknown and unauthorized third parties the Private Information of Plaintiffs and the Class.

162. Defendant allowed unauthorized and unknown third parties to access and examine the Private Information of Plaintiffs and the Class, by way of Defendant's failure to protect the Private Information.

163. The unauthorized exposure to unauthorized third parties of the Private Information of Plaintiffs and the Class is highly offensive to a reasonable person, especially because of the highly sensitive nature of the data affected.

164. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and the Class disclosed their Private Information to Defendant as part of Plaintiffs' and the Class's relationships with Defendant, but privately with an intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

165. Because of the intrusion, Plaintiffs' and Class Members' data was exposed to notorious cybercriminals and other identity thieves whose mission it is to misuse PII and PHI.

166. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person and it further represents a disclosure of private facts to the public.

167. Defendant acted with a knowing and intentional state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

168. Moreover, due to the highly foreseeable nature of data breaches and the harm inherent therefrom, Defendant's failure to implement reasonable security measures was done with substantial certainty of the harm that that would and did follow.

169. Because Defendant acted with this knowing state of mind, it was substantially certain that its inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and the Class.

170. As a proximate result of the above acts and omissions of Defendant, the Private Information of Plaintiffs and the Class was disclosed to third parties without authorization, causing Plaintiffs and the Class to suffer damages.

171. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class in that the Private Information maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs or Class Members.

COUNT VII
MISSOURI MERCHANDISE PRACTICES ACT
Mo. Rev. Stat. §§ 407.010, et seq.
(On behalf of Plaintiff and the Class)

172. Plaintiffs and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

173. Defendant is a “person” as defined by Mo. Rev. Stat. § 407.010(5).

174. Defendant engaged in “sales” of and “advertisements” for “merchandise” in Missouri and engaged in trade or commerce directly or indirectly affecting the people of Missouri, as defined by Mo. Rev. Stat. § 407.010(1), (4), (6) and (7).

175. Defendant engaged in unlawful, unfair, and deceptive acts and practices, in connection with the sale or advertisement of merchandise in trade or commerce, in violation of Mo. Rev. Stat. § 407.020(1), including:

- a. Failing to implement and maintain reasonable security and privacy measures to Plaintiff and Class Members' Private Information, which was a direct and proximate cause of the Data Breach; Electronically Filed - St Louis County - May 14, 2025 - 12:53 PM
- b. Failing to identify and remediate foreseeable security and privacy risks and properly improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Class Members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' Private information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff and Class Members' Private Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

176. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

- i. For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and Plaintiff's counsel as Class Counsel;
- ii. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information;
- iii. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;
- iv. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
- v. Ordering Defendant to pay for not less than three years of credit monitoring services and/or identity theft protection for Plaintiff and Class Members;
- vi. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- vii. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- viii. Pre- and post-judgment interest on any amounts awarded; and
- ix. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all claims so triable.

Dated: May 29, 2025

Respectfully Submitted,

/s/ John F. Garvey

John F. Garvey, #35879 (MO)

Colleen Garvey, #72809 (MO)

STRANCH, JENNINGS & GARVEY, PLLC

701 Market Street, Suite 1510 St. Louis, MO
63101

Tel: (314) 390-6750

jgarvey@stranchlaw.com

cgarvey@stranchlaw.com

J. Gerard Stranch, IV*

Grayson Wells*

STRANCH, JENNINGS & GARVEY, PLLC

The Freedom Center

223 Rosa L. Parks Avenue, Suite 200

Nashville, TN 37203

Tel: (615) 254-8801

gstranch@stranchlaw.com

gwells@stranchlaw.com

*Counsel for Plaintiff and
The Proposed Class*

**Pro Hac Vice application forthcoming*

In the
CIRCUIT COURT
Of St. Louis County, Missouri



For File Stamp Only

Robin Willis, individually and on behalf of all others similarly situated
Plaintiff/Petitioner

Date

Case Number

vs.

American Multispecialty Group, Inc., d/b/a Esse Health
Defendant/Respondent

Division

REQUEST FOR APPOINTMENT OF PROCESS SERVER

Comes now Plaintiff, pursuant
Requesting Party

to Local Rule 28, and at his/her/its own risk requests the appointment of the Circuit Clerk of
H&H Investigations, 432 Evergreen, St. Louis, MO 63119 314-225-8114

Name of Process Server Address Telephone

Name of Process Server Address or in the Alternative Telephone

Name of Process Server Address or in the Alternative Telephone

Natural person(s) of lawful age to serve the summons and petition in this cause on the below
named parties. This appointment as special process server does not include the authorization
to carry a concealed weapon in the performance thereof.

SERVE:

American Multispecialty Group, Inc.
Name
12655 Olive Blvd.
Address
St. Louis, MO 63141
City/State/Zip

SERVE:

Name
Address
City/State/Zip

SERVE:

Name
Address
City/State/Zip

SERVE:


Name
Address
City/State/Zip

Appointed as requested:

JOAN M. GILMER, Circuit Clerk

By _____
Deputy Clerk

Date


Signature of Attorney/Plaintiff/Petitioner
35879
Bar No.
701 Market St., Ste. 1510, St. Louis, MO 63101
Address
(314) 390-6750
Phone No. Fax No.

Local Rule 28. SPECIAL PROCESS SERVERS

(1) Any Judge may appoint a Special Process Server in writing in accordance with the law and at the risk and expense of the requesting party except no special process server shall be appointed to serve a garnishment [except as allowed by Missouri Supreme Court Rule 90.03(a)].

This appointment as Special Process Server does not include the authorization to carry a concealed weapon in the performance thereof.

(2) The Circuit Clerk may appoint a natural person other than the Sheriff to serve process in any cause in accordance with this subsection;

(A) Appointments may list more than one server as alternates.

(B) The appointment of a person other than the Sheriff to serve process shall be made at the risk and expense of the requesting party.

(C) Any person of lawful age, other than the Sheriff, appointed to serve process shall be a natural person and not a corporation or other business association.

(D) No person, other than the Sheriff, shall be appointed to serve any order, writ or other process which requires any levy, seizure, sequestration, garnishment, [except as allowed by Missouri Supreme Court Rule 90.03(a)], or other taking.

(E) Requests for appointment of a person other than the Sheriff to serve process shall be made on a "Request for Appointment of Process Server" electronic form, which may be found on the Court's Web Site,
<https://stlcourtscourts.com/forms/associate-civil/request-process-server/>

(F) This appointment as Special Process Server does not include the authorization to carry a concealed weapon in the performance thereof.

SERVICE RETURN

Any service by the St. Louis County Sheriff's Office shall be scanned into the courts case management system. Any service by another Sheriff or a Special Process Server or any other person authorized to serve process shall return to the attorney or party who sought service and the attorney shall file the return electronically to the Circuit Clerk.



Summons in Civil Case

IN THE 21ST JUDICIAL CIRCUIT, ST. LOUIS COUNTY, MISSOURI

Judge or Division: MARY ELIZABETH OTT	Case Number: 25SL-CC05839	(Date File Stamp for Return)
Plaintiff/Petitioner: ROBIN WILLIS	Plaintiff's/Petitioner's Attorney/Address JOHN FRANCIS GARVEY JR 701 MARKET ST SUITE 1510 ST LOUIS, MO 63101	
Defendant/Respondent: AMERICAN MULTISPECIALTY GROUP, INC. DBA: ESSE HEALTH	Court Address: ST LOUIS COUNTY COURT BUILDING 105 SOUTH CENTRAL AVENUE CLAYTON, MO 63105	
Nature of Suit: CC Breach of Contract		

The State of Missouri to: **AMERICAN MULTISPECIALTY GROUP, INC.**
Alias:
DBA: ESSE HEALTH

12655 OLIVE BLVD., FLOOR 4
ST. LOUIS, MO 63141

You are summoned to appear before this court and to file your pleading to the petition, a copy of which is attached, and to serve a copy of your pleading upon the attorney for plaintiff/petitioner at the above address all within 30 days after receiving this summons, exclusive of the day of service. If you fail to file your pleading, judgment by default may be taken against you for the relief demanded in the petition.

COURT SEAL OF



ST. LOUIS COUNTY

02-JUN-2025

Date

/S/ Adam Dockery

Clerk

Further Information:

AD

Officer's or Server's Return

Note to serving officer: Service should be returned to the court within 30 days after the date of issue.

I certify that I have served the above Summons by: (check one)

- ☐ delivering a copy of the summons and petition to the defendant/respondent.
- ☐ leaving a copy of the summons and petition at the dwelling house or usual place of abode of the defendant/respondent with _____, a person at least 18 years of age residing therein.
- ☐ (for service on a corporation) delivering a copy of the summons and petition to: _____ (name) _____ (title).
- ☐ other: _____.

Served at _____ (address)
in _____ (County/City of St. Louis), MO, on _____ (date)
at _____ (time).

Printed Name of Officer or Server

Signature of Officer or Server

Must be sworn before a notary public if not served by an authorized officer.

Subscribed and sworn to before me on _____ (date).

(Seal)

My commission expires: _____
Date Notary Public

Service Fees (if applicable)

Summons	\$ _____
Non Est	\$ _____
Sheriff's Deputy Salary	
Supplemental Surcharge	\$ 10.00
Mileage	\$ _____ (_____ miles @ \$. _____ per mile)
Total	\$ _____

A copy of the summons and petition must be served on **each** defendant/respondent. For methods of service on all classes of suits, see Supreme Court Rule 54.

THE CIRCUIT COURT OF ST. LOUIS COUNTY, MISSOURI

Twenty First Judicial Circuit

NOTICE OF ALTERNATIVE DISPUTE RESOLUTION SERVICES

Purpose of Notice

As a party to a lawsuit in this court, you have the right to have a judge or jury decide your case. However, most lawsuits are settled by the parties before a trial takes place. This is often true even when the parties initially believe that settlement is not possible. A settlement reduces the expense and inconvenience of litigation. It also eliminates any uncertainty about the results of a trial.

Alternative dispute resolution services and procedures are available that may help the parties settle their lawsuit faster and at less cost. Often such services are most effective in reducing costs if used early in the course of a lawsuit. Your attorney can aid you in deciding whether and when such services would be helpful in your case.

Your Rights and Obligations in Court Are Not Affected By This Notice

You may decide to use an alternative dispute resolution procedure if the other parties to your case agree to do so. In some circumstances, a judge of this court may refer your case to an alternative dispute resolution procedure described below. These procedures are not a substitute for the services of a lawyer and consultation with a lawyer is recommended. Because you are a party to a lawsuit, you have obligations and deadlines which must be followed whether you use an alternative dispute resolution procedure or not. **IF YOU HAVE BEEN SERVED WITH A PETITION, YOU MUST FILE A RESPONSE ON TIME TO AVOID THE RISK OF DEFAULT JUDGMENT, WHETHER OR NOT YOU CHOOSE TO PURSUE AN ALTERNATIVE DISPUTE RESOLUTION PROCEDURE.**

Alternative Dispute Resolution Procedures

There are several procedures designed to help parties settle lawsuits. Most of these procedures involve the services of a neutral third party, often referred to as the “neutral,” who is trained in dispute resolution and is not partial to any party. The services are provided by individuals and organizations who may charge a fee for this help. Some of the recognized alternative dispute resolutions procedures are:

(1) Advisory Arbitration: A procedure in which a neutral person or persons (typically one person or a panel of three persons) hears both sides and decides the case. The arbitrator’s decision is not binding and simply serves to guide the parties in trying to settle their lawsuit. An arbitration is typically less formal than a trial, is usually shorter, and may be conducted in a private setting at a time mutually agreeable to the parties. The parties, by agreement, may select the arbitrator(s) and determine the rules under which the arbitration will be conducted.

(2) Mediation: A process in which a neutral third party facilitates communication between the parties to promote settlement. An effective mediator may offer solutions that have not been considered by the parties or their lawyers. A mediator may not impose his or her own judgment on the issues for that of the parties.

(3) Early Neutral Evaluation (“ENE”): A process designed to bring the parties to the litigation and their counsel together in the early pretrial period to present case summaries before and receive a non-binding assessment from an experienced neutral evaluator. The objective is to promote early and meaningful communication concerning disputes, enabling parties to plan their cases effectively and assess realistically the relative strengths and weaknesses of their positions. While this confidential environment provides an opportunity to negotiate a resolution, immediate settlement is not the primary purpose of this process.

(4) Mini-Trial: A process in which each party and their counsel present their case before a selected representative for each party and a neutral third party, to define the issues and develop a basis for realistic settlement negotiations. The neutral third party may issue an advisory opinion regarding the merits of the case. The advisory opinion is not binding.

(5) Summary Jury Trial: A summary jury trial is a non binding, informal settlement process in which jurors hear abbreviated case presentations. A judge or neutral presides over the hearing, but there are no witnesses and the rules of evidence are relaxed. After the “trial”, the jurors retire to deliberate and then deliver an advisory verdict. The verdict then becomes the starting point for settlement negotiations among the parties.

Selecting an Alternative Dispute Resolution Procedure and a Neutral

If the parties agree to use an alternative dispute resolution procedure, they must decide what type of procedure to use and the identity of the neutral. As a public service, the St. Louis County Circuit Clerk maintains a list of persons who are available to serve as neutrals. The list contains the names of individuals who have met qualifications established by the Missouri Supreme Court and have asked to be on the list. The Circuit Clerk also has Neutral Qualifications Forms on file. These forms have been submitted by the neutrals on the list and provide information on their background and expertise. They also indicate the types of alternative dispute resolution services each neutral provides.

A copy of the list may be obtained by request in person and in writing to: Circuit Clerk, Office of Dispute Resolution Services, 105 South Central Avenue, 5th Floor, Clayton, Missouri 63105. The Neutral Qualifications Forms will also be made available for inspection upon request to the Circuit Clerk.

The List and Neutral Qualification Forms are provided only as a convenience to the parties in selecting a neutral. The court cannot advise you on legal matters and can only provide you with the List and Forms. You should ask your lawyer for further information.



OFFICE OF THE CIRCUIT CLERK

Missouri's 21st Judicial Circuit, St. Louis County

Civil Department

105 South Central Avenue, Clayton, MO 63105

Hours: Monday through Friday 8:00 A.M. to 5:00 P.M.

Phone: 314-615-8029

SPECIAL NEEDS: If you have special needs addressed by the Americans With Disabilities Act. Please notify the Office of the Circuit Clerk at 314-615-8029. FAX 314-615-8739, email at SLCADA@courts.mo.gov, or through Relay Missouri by dialing 711 Or 800-735-2966, at least three business days in advance of the court proceeding.